

Federal Bureau of Investigation (FBI) Solicitation  
Channelers to the FBI's Criminal Justice Information Services (CJIS) Division for  
National Noncriminal Justice Fingerprint Submissions

SECTION A – SF-33 (See Attached)

## SECTION B – SUPPLIES OR SERVICES AND PRICE/COST

### Supplies or Services

The purpose of this solicitation is to select one or multiple Contractors that will provide processing services for authorized national noncriminal justice fingerprint submissions from:

- Authorized Recipients
- Individuals seeking their own criminal history record pursuant to Departmental Order (DO) 556-73.

The Contractors will obtain contracts with Authorized Recipients and/or agreements with authorized individuals, receive national noncriminal justice applicant fingerprint submissions and collect associated fees, ensure fingerprint submissions are properly and adequately completed, electronically forward fingerprint submissions to the FBI's CJIS Division for national noncriminal justice criminal history record checks, receive electronic record check results for dissemination to Authorized Recipients and/or authorized individuals, and perform other administrative tasks pursuant to the National Crime Prevention and Privacy Compact Council's (Council's) Outsourcing Rule and Standard. The number of Contractors that will eventually be approved is unknown at this time; however, the FBI will strive to strike a balance between the number of Contractors it has the capability to administer (i.e. the number of connections the FBI may reasonably establish during this initiative and audit) and the number of Contractors needed to effectively and efficiently serve the needs of the FBI, Authorized Recipients, and authorized individuals.

One or multiple Contractors will be selected based on this solicitation to provide services to the FBI, Authorized Recipients, and authorized individuals. The number of Contractors selected initially is dependent on the number of connections and the number of audits the FBI can reasonably conduct during the upcoming year(s).

### Price/Cost

No price or cost proposal is requested for this solicitation. The FBI will not be issuing a Purchase Order for the award of this contract; however, the FBI will issue a signed SF-33 Solicitation, Offer, and Award.

### Contract Term

Contractors will be selected for a one-year base period with four exercisable one-year option periods. The contract will be executed by the SF-33 Solicitation, Offer, and Award. However, the Government reserves the right to terminate the contract at any time for the convenience of the Government and to add additional Channelers during the term of this contract as the Government deems necessary.

Contractors may terminate the contract, with a 60 day prior written notice to the FBI, with its intent to discontinue or opt out at any time. Such notification and withdrawal from the contract will in no way reflect negatively upon the contractor's organization.

## SECTION C – DESCRIPTION/SPECIFICATION/STATEMENT OF WORK

### Statement of Work Channelers to the FBI's CJIS Division for National Noncriminal Justice Fingerprint Submissions

#### 1. INTRODUCTION

##### 1.1 BACKGROUND

The FBI's, CJIS Division, Clarksburg, West Virginia, provides positive identification services based on fingerprints, and maintains a national repository of fingerprint identification and criminal history record information. Since 1999, the FBI has performed identification services using the Integrated Automated Fingerprint Identification System (IAFIS). The IAFIS is designed to process fingerprint information electronically.

The National Crime Prevention and Privacy Compact Act of 1998 (Compact) (title 42, United States Code (U.S.C.), sections 14611-14616) provides a legal framework for the cooperative exchange of criminal history records between Federal and state entities for noncriminal justice purposes. The Compact established a fifteen-member Council, whose members are appointed by the United States Attorney General (AG), to promulgate rules, procedures, and standards governing the use of the Interstate Identification Index (III) criminal history record information (CHRI) for noncriminal justice purposes.

The Council published the "Outsourcing of Noncriminal Justice Administrative Functions" Interim Final Rule (IFR) and two "Security and Management Control Outsourcing Standards" (Outsourcing Standards) in the Federal Register on December 16, 2004. See 69 FR 75243 and 69 FR 75350, respectively. The Council adopted the IFR as a final rule (rule) and published a combined Outsourcing Standard in the Federal Register on December 15, 2005. See 70 FR 74200 and 70 FR 74373, respectively. The rule permits an Authorized Recipient of CHRI to outsource noncriminal justice administrative functions relating to the processing of CHRI to a third party, subject to appropriate controls. The rule states that contracts or agreements providing for authorized outsourcing "shall incorporate by reference a security and management control outsourcing standard approved by the Council after consultation with the United States AG." In November 2009, the Council decided to bifurcate the Outsourcing Standard to create one strictly for Channeler Contractors (Outsourcing Standard for Channelers) and the other for non-Channeler Contractors (Outsourcing Standard for Non-Channelers). The Council periodically updates the Outsourcing Standard for Channelers and the most current version is dated November 3, 2010.

The FBI originally published a Request For Proposal (RFP) in 2006 in which it awarded 19 companies a contract to serve as Channelers. The RFP was a one-year base year award with four exercisable one-year option periods. At the current time, the FBI holds contracts with 15 FBI-approved Channelers.

RFP #06212005 is set to expire on November 7, 2011. The FBI is publishing a new RFP to select one or multiple Contractors to provide processing services for authorized national noncriminal justice fingerprint submissions to the FBI.

##### 1.2 SCOPE OF WORK

The purpose of this Statement of Work (SOW) is to select one or multiple Contractors. Contractors will obtain contracts with Authorized Recipients and/or agreements with authorized individuals, receive national noncriminal justice applicant fingerprint submissions and collect associated fees, ensure fingerprint submissions are properly and adequately completed, electronically forward fingerprint submissions to the FBI's CJIS Division for national noncriminal justice criminal history record checks, receive electronic record check results for prompt and private dissemination to Authorized Recipients and/or authorized individuals, pursuant to the Council's Outsourcing Rule and

Standard. The number of Contractors that will eventually be selected to perform channeling services is unknown at this time; however, the FBI will strive to strike a balance between the number of Contractors it has the capability to administer (i.e. the number of connections the FBI may reasonably establish during this initiative and audit) and the number of Contractors needed to effectively and efficiently serve the needs of the FBI, Authorized Recipients, and authorized individuals.

Additionally, the United States Department of Justice Order 556-73 (DO 556-73) authorized each subject of an FBI criminal identification record to obtain a copy of his/her own record. The federal regulations pertaining to the DO 556-73 process are found in 28 Code of Federal Regulations (CFR) 16.30-16.34. These regulations establish procedures to be followed should an individual wish to obtain a copy of his/her FBI criminal identification record, upon request, for review and correction purposes, to challenge the information on record, or satisfy certain legal requirements such as a requirement for adopting a child; to satisfy a requirement to live in a foreign country; to satisfy a requirement to work in a foreign country; to satisfy a requirement to travel in a foreign country; and/or other court-related matters.

Contractors designated to request national fingerprint-based noncriminal justice criminal history record background checks on behalf of a noncriminal justice agency (NCJA) [public] or noncriminal justice entity (private) for noncriminal justice purposes shall be eligible for access to FBI-maintained CHRI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All Contractors accessing CHRI shall be subject to the terms and conditions described in the Council's Outsourcing Standard for Channelers.

A Contractor will be responsible for meeting, maintaining and/or exceeding all outlined requirements for all connections needed to transmit fingerprints to the CJIS Division and receive CHRI from the FBI for prompt, private, and secure transmission to Authorized Recipients and/or authorized individuals. Should a Contractor choose to submit for Authorized Recipients and/or authorized individuals, specific technical restrictions and requirements shall be adhered to at all times during the contract period.

All NCJAs accessing FBI-maintained CHRI shall be subject to all pertinent areas of the FBI CJIS Security Policy (attached). Each NCJA that directly accesses FBI criminal justice information (CJI) shall also allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system per authorization of Department of Justice (DOJ) Order 2640.2F.

## 2. APPLICABLE DOCUMENTS

### 2.1 Specifications

- IAFIS Image Quality Specifications – [www.fbi/biospecs.org/docs/EBTS\\_v9\\_2\\_Final\\_20110706.pdf](http://www.fbi/biospecs.org/docs/EBTS_v9_2_Final_20110706.pdf) (Appendix F)
- Electronic Biometric Transmission Specification (EBTS) – [www.fbi/biospecs.org/ebts.html](http://www.fbi/biospecs.org/ebts.html)
- IAFIS Wavelet Scalar Quantization (WSQ) Gray Scale Fingerprint Image Compression Specification – [www.fbi/biospecs.org/docs/WSQ\\_Gray-scale\\_specification\\_version\\_3\\_1\\_Final.pdf](http://www.fbi/biospecs.org/docs/WSQ_Gray-scale_specification_version_3_1_Final.pdf)

### 2.2 Other

- National Crime Prevention and Privacy Compact Act of 1998 (42 U.S.C. 14611-14616)
- 28 CFR Chapter IX
- Rules, Procedures, and Standards promulgated by the Council
  - 12/16/2004 Outsourcing of Noncriminal Justice Administrative Functions IFR - Adopted as a Final Rule on 12/15/2005 and codified at 28 CFR § 906

- The Security and Management Control Outsourcing Standard for Channelers, dated November 3, 2010 (Incorporated by Reference into this Contractual effort)
- Memorandum of Understanding (MOU)
- FBI CJIS Security Policy Version 5.0, dated February 9, 2011

### 3. DEFINITIONS

The following definitions are provided in Section 1.0 of the Council's Outsourcing Standard for Channelers. The definitions are provided in this SOW for reference in providing a response to the RFP.

3.1 Access to CHRI means to view or make use of CHRI obtained from the III System but excludes direct access to the III System by computer terminal or other automated means by Contractors other than those that may be contracted by the FBI or state criminal history record repositories or as provided by title 42, United States Code, section 14614(b).

3.2 Authorized Recipient means (1) a nongovernmental entity authorized by federal statute or federal executive order to receive CHRI for noncriminal justice purposes, or (2) a government agency authorized by federal statute, federal executive order, or state statute which has been approved by the United States AG to receive CHRI for noncriminal justice purposes.

3.3 Authorized Recipient's Information Security Officer means the individual who shall ensure technical compliance with all applicable elements of this Outsourcing Standard for Channelers.

3.4 Chief Administrator, as referred to in Article I(2)(B) of the Compact, means the primary administrator of a Nonparty State's criminal history record repository or a designee of such administrator who is a regular full-time employee of the repository.

3.5 CHRI, as referred to in Article I(4) of the Compact, means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, or other formal criminal charges, and any disposition arising there from, including acquittal, sentencing, correctional supervision, or release; but does not include identification information such as fingerprint records if such information does not indicate involvement of the individual with the criminal justice system.

3.6 Criminal History Record Check, for purposes of this Outsourcing Standard for Channelers only, means an authorized noncriminal justice fingerprint-based search of a state criminal history record repository and/or the FBI system.

3.7 CJIS Systems Agency, as provided in Section 1.4 of the FBI Criminal Justice Information Services (CJIS) Division's Advisory Policy Board Bylaws, means a criminal justice agency which has overall responsibility for the administration and usage of CJIS Division Programs within a state, district, territory, or foreign country. This includes any federal agency that meets the definition and provides services to other federal agencies and/or whose users reside in multiple states or territories.

3.8 CJIS Systems Officer, as provided in Section 1.5 of the CJIS Advisory Policy Board Bylaws, means the individual employed by the CJIS Systems Agency who is responsible for monitoring system use, enforcing system discipline and security, and assuring that CJIS operating procedures are followed by all users as well as other related duties outlined by the user agreements with the FBI's CJIS Division. (This title was formerly referred to as the Control Terminal Officer or the Federal Service Coordinator).

3.9 Compact Officer, as provided in Article I(2) of the Compact, means (A) with respect to the Federal Government, an official [FBI Compact Officer] so designated by the Director of the FBI [to administer and enforce the

compact among federal agencies], or (B) with respect to a Party State, the chief administrator of the State's criminal history record repository or a designee of the chief administrator who is a regular full-time employee of the repository.

3.10 Contractor means a government agency, a private business, non-profit organization or individual, that is not itself an Authorized Recipient with respect to the particular noncriminal justice purpose, who has entered into a contract with an Authorized Recipient to perform channeler functions requiring access to CHRI. Under the Outsourcing Standard for Channelers, a Contractor serves as a Channeler and has direct connectivity to the CJIS Wide Area Network (WAN) for the purpose of electronic submission of fingerprints to and the receipt of CHRI from the FBI on behalf of an Authorized Recipient.

3.11 Contractor's Security Officer means the individual accountable for the management of the Contractor's security program.

3.12 Dissemination means the disclosure of CHRI by an Authorized Recipient to an authorized Contractor, or by the Contractor to another Authorized Recipient consistent with the Contractor's responsibilities and with limitations imposed by federal and state laws, regulations, and standards as well as rules, procedures, and standards established by the Council and the United States AG.

3.13 Noncriminal Justice Administrative Functions means the routine noncriminal justice administrative functions relating to the processing of CHRI, to include but not limited to the following:

- (1) Making fitness determinations/recommendations
- (2) Obtaining missing dispositions
- (3) Disseminating CHRI as authorized by federal statute, federal executive order, or state statute approved by the United States AG
- (4) Other authorized activities relating to the general handling, use, and storage of CHRI

3.14 Noncriminal Justice Purposes, as provided in Article I(18) of the Compact, means uses of criminal history records for purposes authorized by federal or state law other than purposes relating to criminal justice activities, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

3.15 Outsourcing Standard for Channelers means a document approved by the Council after consultation with the United States AG which is to be incorporated by reference into a contract between an Authorized Recipient and a Contractor. The Outsourcing Standard for Channelers authorizes access to CHRI, limits the use of the information to the purposes for which it is provided, prohibits retention and/or dissemination except as specifically authorized, ensures the security and confidentiality of the information, provides for audits and sanctions, provides conditions for termination of the contract, and contains such other provisions as the Council may require.

3.16 Physically Secure Location means a location where access to CHRI can be obtained, and adequate protection is provided to prevent any unauthorized access to CHRI.

3.17 Positive Identification, as provided in Article I(20) of the Compact, means a determination, based upon a comparison of fingerprints<sup>1</sup> or other equally reliable biometric identification techniques, that the subject of a record search is the same person as the subject of a criminal history record or records indexed in the CHRI System. Identifications based solely upon a comparison of subjects' names or other non-unique identification characteristics or numbers, or combinations thereof, shall not constitute positive identification.

---

<sup>1</sup> The Compact Council currently defines positive identification for noncriminal justice purposes as identification based upon a qualifying ten-rolled or qualifying ten-flat fingerprint submission. Further information concerning positive identification may be obtained from the FBI Compact Council office.

3.18 Public Carrier Network means a telecommunications infrastructure consisting of network components that are not owned, operated, and managed solely by the agency using that network, i.e., any telecommunications infrastructure which supports public users other than those of the agency using that network. Examples of a public carrier network include but are not limited to the following: dial-up and Internet connections, network connections to Verizon, network connections to AT&T, ATM Frame Relay clouds, wireless networks, wireless links, and cellular telephones. A public carrier network provides network services to the public; not just to the single agency using that network.

3.19 Security Violation means the failure to prevent or failure to institute safeguards to prevent access, use, retention, or dissemination of CHRI in violation of: (A) federal or state law, regulation, or executive order; or (B) a rule, procedure, or standard established by the Council and the United States AG.

#### 4. CONTRACTOR RESPONSIBILITIES (AS PROVIDED IN THE OUTSOURCING STANDARD FOR CHANNELERS), AUDITS, AND SANCTIONS APPLICABLE WHEN AUTHORIZED AGENCIES CONTRACT CHANNELING FUNCTIONS

The following Contractor responsibilities are predominately restated from the Council's Outsourcing Standard for Channelers. The Contractor's responsibilities are provided in this SOW for reference in providing a response to the RFP, to include delivering a Security Program Plan and Contingency Plan 30 days prior to the FBI Audit.

##### 4.1 Policy

4.1.1 The Contractor and its employees shall comply with all federal and state laws, regulations, and standards (including the most current version of the FBI CJIS Security Policy) as well as with rules, procedures, and standards established by the Council and the United States AG.

4.1.2 The FBI CJIS Security Policy, version 5.0, is incorporated by reference and made part of the Outsourcing Standard for Channelers.

4.1.3 Compliance with the FBI CJIS Security Policy shall be adhered to at all times and within all sections contained in the RFP.

4.1.4 Compliance with the Outsourcing Standard for Channelers shall be adhered to at all times and within all sections contained in the RFP.

##### 4.2 Security

The Contractor shall develop, document, administer, and maintain a Security Program (Physical, Personnel, and Information Technology) to fully comply with the Council's Outsourcing Rule, the most current version of the Outsourcing Standard for Channelers requirements, the most current version of the FBI CJIS Security Policy, and any other document as required by the FBI. The Security Program is subject to approval by the FBI CJIS Division and review by the Authorized Recipient and the Compact Officer/Chief Administrator. Additional guidance related to the limited interaction with criminal justice information, to include CHRI, can be found in Appendix J (attached) of the current version of the FBI CJIS Security Policy. During the audit, provisions will be made to update the Security Program to address security violations and to ensure changes in policies and standards, as well as changes in federal and state law, are incorporated.

##### 4.2.1 Training

4.2.1.1 The Contractor shall develop a Security Training Program for all Contractor personnel with access to CHRI prior to their appointment/assignment, except when the training requirement is required and documentation retained by the Authorized Recipient. The Contractor's Security Training Program shall be subject to review and written approval by the FBI CJIS Division. Immediate training shall be provided upon receipt of notice from the Compact Officer/Chief Administrator on any changes to federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Council and the United States AG. The Contractor shall certify in writing to the FBI CJIS Division that biennial refresher training was completed for those Contractor personnel with access to CHRI, following the training.

#### 4.2.2 Site Security

4.2.2.1 The Contractor's site shall abide by the physical protection policy and procedures as directed in the FBI CJIS Security Policy.

#### 4.2.3 Dissemination

4.2.3.1 Only employees of the Contractor, employees of the Authorized Recipient, and such other persons as may be granted authorization by the Authorized Recipient, shall be permitted access to the IAFIS system through an FBI issued Originating Agency Identifier (ORI) number.

4.2.3.2 Access to the system shall be available only for official purposes consistent with the contract between the Contractor and the Authorized Recipient. Any dissemination of CHRI data to authorized employees of the Contractor is to be for official purposes only.

4.2.3.3 Information contained in or about the IAFIS system will not be provided to agencies other than the Authorized Recipient or another entity which is specifically designated in the contract.

4.2.3.4 The Contractor shall not disseminate CHRI without the consent of the Authorized Recipient, and as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Council and the United States AG.

4.2.3.5 An up-to-date log concerning dissemination of CHRI shall be maintained by the Contractor for a minimum one year retention period. This log must clearly identify: (A) the Authorized Recipient and the secondary recipient, with assigned unique identifiers, (B) the record disseminated, (C) the date of dissemination, (D) the statutory authority for dissemination, and (E) the means of dissemination.

4.2.3.6 The Contractor shall maintain CHRI only for the period of time necessary to fulfill their contractual obligations. CHRI disseminated by a Contractor to an Authorized Recipient via an authorized Web site shall remain on such Web site only for the time necessary to meet the Authorized Recipient's requirements but in no event shall that time exceed 30 calendar days. CHRI successfully received by the Authorized Recipient, regardless of mode of transmission, shall be destroyed by the Contractor immediately after confirmation of successful receipt by the Authorized Recipient. The manner of, and time frame for, CHRI disseminated by a Contractor to an Authorized Recipient shall be specified in the contract or agreement.

4.2.3.7 If CHRI is disseminated in an electronic format, the Contractor shall protect against any unauthorized persons gaining access to the equipment and any of the data. In no event shall responses containing CHRI be disseminated other than governed by the Outsourcing Standard for Channelers or more stringent contract requirements.

4.2.3.8 All access attempts are subject to recording and routine review for detection of inappropriate or illegal activity.

#### 4.2.4 Personnel Security

4.2.4.1 The FBI shall conduct criminal history record checks of Contractor personnel, to include approved sub-contractor, personnel having access to CHRI. Criminal history record checks must be completed prior to accessing CHRI under the contract.

4.2.4.2 The Contractor shall ensure that each employee performing work under the contract is aware of the requirements of the Outsourcing Standard for Channelers and the state and federal laws governing the security and integrity of CHRI. The Contractor shall confirm in writing to the FBI that each employee has certified in writing that he/she understands the Outsourcing Standard for Channelers requirements and laws that apply to his/her responsibilities. The Contractor shall maintain the employee certification in a file that is subject to review during audits. Employees shall make such certification prior to performing work under the contract.

4.2.4.3 The Contractor shall maintain updated records of personnel who have access to CHRI, update those records within 24 hours when changes to that access occur, and maintain a list of personnel who have successfully completed criminal history record checks. Contractors shall notify the FBI within 24 hours when additions or deletions occur.

4.2.4.4 The Contractor is responsible to set, maintain, and enforce the standards for the selection, supervision, and separation of personnel who have access to CHRI per the requirements of the FBI CJIS Security Policy.

#### 4.2.5 System Security

4.2.5.1 The Contractor's security system shall comply with the FBI CJIS Security Policy in effect at the time the Outsourcing Standard for Channelers is incorporated into the contract and with successor versions of the FBI CJIS Security Policy as updated and notified. The Contractor's network connection to CJIS and all parts of the Contractor's network that have CJIS connectivity shall follow the network encryption and user authentication requirements specified in the FBI CJIS Security Policy.

4.2.5.1.1 If CHRI can be accessed by unauthorized personnel via a Virtual Private Network or the Internet, then the Contractor shall protect the CHRI with firewall-type devices to prevent such unauthorized access. These devices shall implement a minimum firewall profile as specified by the FBI CJIS Security Policy in order to provide a point of defense and a controlled and audited access to CHRI, both from inside and outside the networks.

4.2.5.1.2 The Contractor shall ensure that data is encrypted pursuant to the requirements in the FBI CJIS Security Policy whenever passing CHRI through a shared public carrier network.

4.2.5.2 The Contractor shall provide for the secure storage and disposal of all hard copy and media associated with the system to prevent access by unauthorized personnel.

4.2.5.2.1 The Contractor shall ensure that CHRI is stored in accordance with the FBI CJIS Security Policy.

4.2.5.2.2 It is the responsibility of the Authorized Recipient to ensure that a procedure is in place for sanitizing all fixed storage media (e.g., disks, drives, backup storage) at the completion of the contract and/or before it is returned for maintenance, disposal, or reuse.

4.2.5.2.3 It is the responsibility of the Authorized Recipient to ensure that a procedure is in place for the disposal or return of all media.

4.2.5.3 To prevent and/or detect unauthorized access to CHRI in transmission or storage, each Authorized Recipient, Contractor, or Sub-Contractor must be assigned a unique identifier.

4.2.5.4 The Contractor's system shall be supported by a documented contingency plan as defined by in the FBI CJIS Security Policy and approved by the FBI.

4.2.5.5 The Contractor shall ensure that the same fingerprint images are not used for more than one submission per individual, specifically in case of fingerprint quality rejects.

#### 4.2.6 Security Violations

4.2.6.1 The Contractor shall develop and maintain a written policy for discipline of Contractor employees who violate the security provisions of the contract, which includes the Outsourcing Standard for Channelers that is incorporated by reference, and the FBI CJIS Security Policy.

4.2.6.1.1 Pending investigation, the Contractor shall, upon detection or awareness, suspend any employee who commits a security violation from assignments in which he/she has access to CHRI under the contract.

4.2.6.1.2 The Contractor shall immediately (within four hours) notify the Authorized Recipient and the FBI of any security violation to include unauthorized access to CHRI. Within five calendar days of such notification, the Contractor shall provide the Authorized Recipient and the FBI a written report documenting such security violation, any corrective actions taken by the Contractor to resolve such violation, and the date, time, and summary of the prior notification.

4.2.6.2 The contract is subject to termination by the Authorized Recipient for (1) security violations involving CHRI obtained pursuant to the contract and (2) the Contractor's failure to notify the Authorized Recipient of any security violation or to provide a written report concerning such violation.

4.2.6.3 If the Contractor refuses to or is incapable of taking corrective actions to successfully resolve a security violation, the Authorized Recipient and/or the FBI shall terminate the contract.

4.2.6.4 Notwithstanding the actions taken by the State Compact Officer or the FBI Compact Officer, if the Authorized Recipient fails to provide a written report notifying the State Compact Officer/Chief Administrator or the FBI Compact Officer of a security violation, or refuses to or is incapable of taking corrective action to successfully resolve a security violation, the Council or the United States AG may suspend or terminate the exchange of CHRI with the Authorized Recipient pursuant to 28 CFR § 906.2(d).

4.2.6.5 If the exchange of CHRI is suspended, it may be reinstated after satisfactory written assurances have been provided to the Council Chairman or the United States AG by the Compact Officer/Chief Administrator, the Authorized Recipient and the Contractor that the security violation has been resolved. If the exchange of CHRI is terminated, the Contractor's records (including media) containing CHRI shall be deleted or returned in accordance with the provisions and time frame as specified by the Authorized Recipient.

4.2.6.6 The Authorized Recipient and/or the Contractor shall provide written notice (through the State Compact Officer/Chief Administrator if applicable) to the FBI Compact Officer of the following: (1) the termination of a contract for security violations, (2) security violations involving the unauthorized access to CHRI, and (3) the Contractor's name and unique identification number (or Authorized Recipient name[s]), the nature of the security violation, whether the violation was intentional, and the number of times the violation occurred.

4.2.6.7 The Compact Officer/Chief Administrator, Council, and the United States AG reserve the right to investigate or decline to investigate any report of unauthorized access to CHRI.

#### 4.3 Audits

The following audit provisions are predominately restated from the Council's Outsourcing Standard for Channelers. The audit provisions are provided in this SOW for reference in providing a response to the RFP.

4.3.1 The Contractor shall make its facilities available for announced and unannounced audits performed by the Authorized Recipient, the state, or the FBI on behalf of the Council. Such facilities are also subject to triennial audits by the state and the FBI on behalf of the Council. An audit may also be conducted on a more frequent basis.

4.3.2 The FBI Compact Officer, Council, and the United States AG reserve the right to conduct a final audit of a Contractor's operations and system following termination and/or conclusion of the contract(s) with the FBI.

4.3.3 The Contractor shall be subject to an FBI audit within 90 days of the date the Contractor first receives CHRI under the terms of the Contract and, at a minimum, a triennial audit with the first of such audits to be conducted within one year of the date the Contractor first receives CHRI under the terms of the contract.

4.3.4 The Contractor shall provide all logs required to be maintained by a Contractor as listed in the Outsourcing Standard for Channelers to the FBI during announced and unannounced audits, to include but not limited to, dissemination of CHRI.

#### 5. CONTRACTOR RESPONSIBILITIES (AS PROVIDED IN THE OUTSOURCING STANDARD FOR CHANNELERS), AUDITS, AND SANCTIONS APPLICABLE WHEN INDIVIDUALS CONTRACT CHANNELING FUNCTIONS PURSUANT TO DO 556-73

##### 5.1 Policy

5.1.1 The Contractor and its employees shall comply with all federal and state laws, regulations, and standards (including the most current version of the FBI CJIS Security Policy) as well as with rules, procedures, and standards established by the Council and the United States AG.

5.1.2 A Contractor, with the intention of processing DO 556-73 requests, is expected to follow the same regulatory and policy requirements regarding the receipt of the DO Request Form, obtaining a complete set of fingerprints, and collecting the appropriate fee from the individual.

5.1.3 A Contractor shall be required to maintain a DO Request Form (to be provided by the FBI following award) with each DO 556-73 request from each individual seeking a national criminal history record check on him or herself.

5.1.4 A Contractor shall retain each DO Request Form with the original signature from each individual, for a period of three (3) years or upon termination of the contract with the FBI, whichever is shorter.

5.1.5 A Contractor must destroy all DO Request Forms at the end of the mandatory retention period in accordance with the provisions of the most current versions of the Outsourcing Standard for Channelers and the FBI CJIS Security Policy for fixed storage media and disposal of all non-fixed storage media of CHRI.

5.1.6 A Contractor submitting a DO 556-73 request for an individual must have the individual's fingerprints captured by a law enforcement agency or the Contractor only. Individuals are not permitted to capture his/her fingerprints on a fingerprint card.

5.1.7 A Contractor submitting fingerprints to the CJIS Division on behalf of an individual pursuant to DO 556-73 and this contract must verify the individual's identity by examining two forms of identification, with at least one of

which must be a government issued photo ID. The individual's mailing address must match at least one form of identification provided to the Contractor and listed on the DO Request Form.

5.1.8 A Contractor shall ensure that a DO 556-73 request that is made through an attorney is submitted on attorney letterhead with both the individual and the attorney signatures, which must contain a request that the CHRI/check result be released to the agent attorney.

5.1.9 A Contractor shall ensure that a DO 556-73 request is not submitted by an individual for employment and/or licensing.

5.1.10 A Contractor shall only submit DO 556-73 requests for U.S. persons (individuals who are a citizen of the U.S. or a lawful permanent resident of the U.S.) not requiring an apostille.

5.1.11 Media protection policy and procedures shall be documented and implemented to ensure that access to electronic and physical media in all forms is restricted to authorized individuals. Procedures shall be defined for securely handling, transporting and storing media.

## 5.2 Security

The Contractor shall develop, document, administer, and maintain a Security Program (Physical, Personnel, and Information Technology) to fully comply with the Council's Outsourcing Rule, the most current version of the Outsourcing Standard for Channelers requirements, the most current version of the FBI CJIS Security Policy, and any other documents as required by the FBI. The Security Program is subject to approval by the FBI CJIS Division and review by the authorized individual(s) and the Compact Officer/Chief Administrator. Additional guidance related to the limited interaction with criminal justice information, to include CHRI, can be found in Appendix J of the current version of the FBI CJIS Security Policy. During the audit, provision will be made to update the Security Program to address security violations and to ensure changes in policies and standards as well as changes in federal and state law are incorporated.

### 5.2.1 Training

5.2.1.1 The Contractor shall develop a Security Training Program for all Contractor personnel with access to CHRI prior to their appointment/assignment. The Contractor's Security Training Program shall be subject to review and written approval by the FBI CJIS Division. Immediate training shall be provided upon receipt of notice from the Compact Officer/Chief Administrator on any changes to federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Council, the United States AG, and the FBI CJIS Security Policy. Annual refresher training shall also be provided. The Contractor shall certify in writing to the FBI CJIS Division that biennial refresher training was completed for those Contractor personnel with access to CHRI.

### 5.2.2 Site Security

5.2.2.1 The Contractor's site shall abide by the physical protection policy and procedures as directed in the FBI CJIS Security Policy.

### 5.2.3 Dissemination

5.2.3.1 Only employees of the Contractor shall be permitted access to the IAFIS system through an FBI issued ORI.

5.2.3.2 Access to the system shall be available only for official purposes consistent with the contract between the Contractor and the authorized individual. Any dissemination of CHRI data to authorized employees of the Contractor is to be for official purposes only.

5.2.3.3 Information contained in or about the IAFIS system will not be provided to another entity.

5.2.3.4 The Contractor shall not disseminate CHRI to anyone other than the authorized individual, and even then such dissemination shall not be contrary to the terms of this Contract, federal and state laws, regulations, and standards or with rules, procedures, and standards established by the Council and the United States AG.

5.2.3.5 An up-to-date log concerning dissemination of CHRI shall be maintained by the Contractor for a minimum one year retention period. This log must clearly identify: (A) the authorized individual and/or the authorized individual's designated agent attorney with assigned unique identifiers, (B) the type of record disseminated (e.g., record or no record), (C) the date of dissemination, (D) the regulatory authority for dissemination (i.e., 28 CFR § 16.32), and (E) the means of dissemination.

5.2.3.6 The Contractor shall maintain CHRI only for the period of time necessary to fulfill its contractual obligations. CHRI disseminated via an authorized Web site shall remain on such Web site only for the time necessary but in no event shall that time exceed 30 calendar days. CHRI successfully disseminated to the authorized individual, regardless of mode of transmission, shall be destroyed by the Contractor immediately after confirmation of successful receipt. The manner of, and time frame for, CHRI disseminated by a Contractor to the authorized individual shall be specified in the agreement.

5.2.3.7 If CHRI is disseminated in an electronic format, the Contractor shall protect against any unauthorized persons gaining access to the equipment and any of the data. In no event shall responses containing CHRI be disseminated other than governed by the Outsourcing Standard for Channelers or more stringent contract requirements. In no event will check results be disseminated in a manner that reasonably facilitates employment or licensing purposes; instead, DO 556-73 checks are specifically for the subject's review and/or correction.

5.2.3.8 All access attempts are subject to recording and routine review for detection of inappropriate or illegal activity.

#### 5.2.4 Personnel Security

5.2.4.1 The FBI shall conduct criminal history record checks of Contractor (and approved Sub-Contractor) personnel having access to CHRI. Criminal history record checks of Contractor personnel having access to FBI-maintained CHRI must be completed by the FBI prior to Contractor access to FBI-maintained CHRI under this contract.

5.2.4.2 The Contractor shall ensure that each employee performing work under the contract is aware of the requirements of the Outsourcing Standard for Channelers and the state and federal laws governing the security and integrity of CHRI. The Contractor shall confirm in writing that each employee has certified in writing that he/she understands the Outsourcing Standard for Channelers requirements and laws that apply to his/her responsibilities. The Contractor shall maintain the employee certification in a file that is subject to review during audits. Employees shall make such certification prior to performing work under the contract.

5.2.4.3 The Contractor shall maintain updated records of personnel who have access to CHRI, update those records within 24 hours when changes to that access occur, and maintain a list of personnel who have successfully completed criminal history record checks. Contractors shall notify the FBI within 24 hours when additions or deletions occur.

5.2.4.4 The Contractor is responsible to set, maintain, and enforce the standards for the selection, supervision, and separation of personnel who have access to CHRI per the requirements of the FBI CJIS Security Policy.

## 5.2.5 System Security

5.2.5.1 The Contractor's security system shall comply with the FBI CJIS Security Policy in effect at the time the Outsourcing Standard for Channelers is incorporated into the contract and with successor versions of the FBI CJIS Security Policy. The Contractor's network connection to CJIS and all parts of the Contractor's network that have CJIS connectivity shall follow the network encryption and user authentication requirements specified in the FBI CJIS Security Policy.

5.2.5.1.1 If CHRI can be accessed by unauthorized personnel via a Wide Area Network/Local Area Network or the Internet, then the Contractor shall protect the CHRI with firewall-type devices to prevent such unauthorized access. These devices shall implement a minimum firewall profile as specified by the FBI CJIS Security Policy in order to provide a point of defense and a controlled and audited access to CHRI, both from inside and outside the networks.

5.2.5.1.2 The Contractor shall ensure that data is encrypted pursuant to the requirements in the FBI CJIS Security Policy whenever passing CHRI through a shared public carrier network.

5.2.5.2 The Contractor shall provide for the secure storage and disposal of all hard copy and media associated with the system to prevent access by unauthorized personnel.

5.2.5.2.1 The Contractor shall ensure that CHRI is stored in accordance with the FBI CJIS Security Policy during the limited time it is in the Contractor's control.

5.2.5.3 To prevent and/or detect unauthorized access to CHRI in transmission or storage, each Contractor, or Sub-Contractor must be assigned a unique identifier.

5.2.5.4 The Contractor's system shall be supported by a documented contingency plan as defined by in the FBI CJIS Security Policy and approved by the FBI.

5.2.5.5 The Contractor shall ensure that the same fingerprint images are not used for more than one submission per individual, specifically in case of fingerprint quality rejects.

## 5.2.6 Security Violations

5.2.6.1 The Contractor shall develop and maintain a written policy for discipline of Contractor employees who violate the security provisions of the contract, which includes the Outsourcing Standard for Channelers that is incorporated by reference, or the FBI CJIS Security Policy.

5.2.6.1.1 Pending investigation, the Contractor shall, upon detection or awareness, suspend any employee who commits a security violation from assignments in which he/she has access to FBI-maintained CHRI under the contract.

5.2.6.1.2 The Contractor shall immediately (within four hours) notify the FBI of any security violation to include unauthorized access to CHRI. Within five calendar days of such notification, the Contractor shall provide the FBI a written report documenting such security violation, any corrective actions taken by the Contractor to resolve such violation, and the date, time, and summary of the prior notification.

5.2.6.2 The contract is subject to termination for (1) security violations involving CHRI obtained pursuant to the contract and (2) the Contractor's failure to notify the FBI of any security violation or to provide a written report concerning such violation.

5.2.6.3 Notwithstanding the actions taken by the State Compact Officer, the Council or the United States AG may suspend or terminate the exchange of CHRI with the Contractor pursuant to 28 CFR § 906.2(d).

5.2.6.4 If the exchange of CHRI is suspended, it may be reinstated after satisfactory written assurances have been provided to the Council Chairman or the United States AG by the Compact Officer/Chief Administrator and the Contractor that the security violation has been resolved. If the exchange of CHRI is terminated, the Contractor's records (including media) containing CHRI shall be deleted.

5.2.6.5 The Contractor shall provide written notice (through the State Compact Officer/Chief Administrator if applicable) to the FBI Compact Officer of the following: (1) the termination of a contract for security violations, (2) security violations involving the unauthorized access to CHRI, and (3) the Contractor's name and unique identification number, the nature of the security violation, whether the violation was intentional, and the number of times the violation occurred.

5.2.6.6 The Compact Officer/Chief Administrator, Council, and the United States AG reserve the right to investigate or decline to investigate any report of unauthorized access to CHRI.

### 5.3 Audits

The following audit provisions are predominately restated from the Council's Outsourcing Standard for Channelers. The audit provisions are provided in this SOW for reference in providing a response to the RFP.

5.3.1 The Contractor shall make its facilities available for announced and unannounced audits performed by the state or the FBI on behalf of the Council. Such facilities are also subject to triennial audits by the state and the FBI on behalf of the Council. An audit may also be conducted on a more frequent basis.

5.3.2 The FBI Compact Officer, Council, and the United States AG reserve the right to conduct a final audit of a Contractor's operations and system following termination and/or conclusion of the contract(s) with the FBI.

5.3.3 The Contractor shall be subject to an FBI audit within 90 days of the date the Contractor first receives CHRI under the terms of the Contract and, at a minimum, a triennial audit with the first of such audits to be conducted within one year of the date the Contractor first receives CHRI under the terms of the contract.

5.3.4 The Contractor shall provide all logs required to be maintained by a Contractor as listed in the Outsourcing Standard for Channelers to the FBI during announced and unannounced audits, to include but not limited to, dissemination of CHRI.

## 6. MISCELLANEOUS PROVISIONS OF THE OUTSOURCING STANDARD

The following miscellaneous provisions are predominately restated from the Council's Outsourcing Standard for Channelers. The miscellaneous provisions are provided in this SOW for reference in providing a response to the RFP.

6.1 The Outsourcing Standard for Channelers does not confer, grant, or authorize any rights, privileges, or obligations to any persons other than the Contractor, the Authorized Recipient, authorized individual, Compact Officer/Chief Administrator (where applicable), CJIS Systems Agency, and the FBI.

6.2 The terms set forth in the Outsourcing Standard for Channelers do not constitute the sole understanding by and between the parties hereto; rather they provide a minimum basis for the security of the IAFIS system and the CHRI accessed there from and it is understood that there may be terms and conditions of the contract between the

Contractor and the Authorized Recipient/authorized individual which impose more stringent requirements upon the Contractor.

6.2.1 More stringent conditions could include additional audits, fees, or security requirements. The Council, Authorized Recipient, authorized individual, and the Compact Officer/Chief Administrator have the explicit authority to require more stringent standards than those contained in the Outsourcing Standard for Channelers.

6.3 The minimum security measures as outlined in the Outsourcing Standard for Channelers may only be modified by the Council. Conformance to such security measures may not be less stringent than stated in the Outsourcing Standard for Channelers without the consent of the Council in consultation with the United States AG.

6.4 The Outsourcing Standard for Channelers may only be modified by the Council and may not be modified by the parties to the contract between the Contractor and the Authorized Recipient/authorized individual without the consent of the Council.

6.5 Appropriate notices, assurances, and correspondence to the FBI Compact Officer, Council, and the United States AG required by Section 8.0 of the Outsourcing Standard for Channelers shall be forwarded by First Class Mail to:

FBI Compact Officer  
Module D-3  
1000 Custer Hollow Road  
Clarksburg, WV 26306

## 7. CONTRACTOR RESPONSIBILITIES IN ADDITION TO THOSE PROVIDED IN THE OUTSOURCING STANDARD

7.1 All Contractor personnel having access to the results of national criminal history record checks shall be citizens of the United States.

7.2 Results of national criminal history record checks will be maintained in a physically secure location(s) within the United States or its territories by the Contractor for the limited time it needs to ensure deliver to the Authorized Recipient or authorized individual and will never be disseminated outside the United States or its territories.

7.3 The Contractor must execute a MOU with the FBI prior to initial configuration and subsequent connection to the FBI CJIS Division. The Contractor shall maintain telecommunication lines and equipment in accordance with the MOU to facilitate CJIS security compliance as stated in the FBI CJIS Security Policy. This MOU may need to be re-executed on an annual basis in order to maintain connectivity to the FBI CJIS Division.

7.4 The Contractor shall execute a contract(s) with an Authorized Recipient(s) and/or agreement with each authorized individual(s) utilizing the Contractor's channeling services. In response to the electronic applicant fingerprint submissions to the FBI's CJIS Division, the Contractor shall receive electronic fingerprint-based criminal history record check results from the FBI and promptly disseminate all criminal history record check results to an Authorized Recipient and/or authorized individual in a manner and time as specified in the contract with an Authorized Recipient and/or agreement with each authorized individual and in accordance with the Outsourcing Standard for Channelers.

7.5 The Contractor shall not enter into a subcontract for any of the services performed under this Contract without obtaining the prior written approval of the FBI Contracting Officer.

7.6 The Contractor shall identify the point of contact (POC) to manage security incidents and violations on their network accessing FBI CJIS data in writing to the FBI Contracting Officer or Contracting Officer's Technical Representative (COTR)/Task Manager (TM).

## 8. CONTRACTOR RESPONSIBILITIES REGARDING PERSONALLY IDENTIFIABLE INFORMATION

8.1 Personally Identifiable Information (PII) is defined as "information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth or mother's maiden name."

8.2 A Contractor is responsible for protecting all PII in its possession and control during the processing of requests. A Contractor shall notify the Authorized Recipient of his/her right (via language approved by the FBI) to report PII breaches to the FBI should he/she believe personal information has been compromised.

8.3 Should a compromise, by accident or on purpose, occur, the Contractor and/or the Authorized Recipient shall immediately report a PII breach to the FBI.

## 9. REQUIREMENTS

The FBI has developed the following requirements that must be met by a Contractor in order to qualify as an approved Channeler Contractor for noncriminal justice applicant fingerprint submissions, as well as authority to receive national criminal history record check results for dissemination to Authorized Recipients and/or authorized individuals.

9.1 The Contractor shall receive authorized noncriminal justice applicant fingerprint submissions, process and transmit to the CJIS Division as digitized electronic records in the formats compliant with the EBTS and the IAFIS WSQ Gray Scale Fingerprint Image Compression Specification for national noncriminal justice criminal history record checks, receive the results of such checks electronically, and expeditiously disseminate the results to Authorized Recipients and/or authorized individuals. (The Contractor is solely responsible for obtaining independent contracts with Authorized Recipients and/or authorized individuals, and each of those contracts must incorporate the most current versions of the Outsourcing Standard for Channelers and the FBI CJIS Security Policy by reference.)

9.1.1 The Contractor shall not retain fingerprint cards and fingerprint images used for submission, unless directed so by the Authorized Recipient, with the exception of DO 556-73 requests, 30 days for Authorized Recipient's under contract. All fingerprints cards and fingerprint images used for DO 556-73 submissions may not be retained for a period longer than 30 calendar days or upon successful dissemination, whichever is shorter. All fingerprint cards and fingerprint images must be destroyed/deleted in a manner consistent with the Outsourcing Standard for Channelers and the FBI CJIS Security Policy.

9.2 The Contractor must maintain direct connectivity to the FBI in accordance with the RFP, the Outsourcing Standard for Channelers and the FBI CJIS Security Policy at all times.

9.3 The Contractor shall ensure that all applicant fingerprint submissions are properly and adequately completed and are being submitted to the CJIS Division in accordance with a federal statute, federal executive order, or a state statute that has been approved by the United States AG and that authorizes fingerprint-based national criminal history record checks. The applicant's fingerprints, name, date of birth, Originating Agency Case "OCA" number, signature and other descriptive data, as well as the reason the applicant is being fingerprinted and the correct statutory authority, must appear in the appropriate areas of the fingerprint submission. The Contractor shall notify the applicant or submitting agency of deficiencies in fingerprint submissions, and shall maintain an audit trail for such submissions.

9.4 The Contractor will be billed by the FBI as set forth below:

Fingerprint-based CHRI Checks			
Service	Fee	Amount Remitted to FBI by CBSPs *	Additional Fee which may be Charged by Contractor
Electronic	\$19.25	\$17.25	Subject to contract with Authorized Recipient
Volunteer	\$15.25	\$13.25	Subject to contract with Authorized Recipient
DO 556-73	\$18.00	\$18.00	Subject to contract with an authorized individual

\*CBSPs – Centralized Billing Service Providers for fingerprint-based CHRI checks

All FBI fees are subject to change. Contractors will be notified of changes ninety (90) days prior to the effective date, either in writing from the FBI or through publication in the Federal Register.

Any additional fee authority shall be pursuant to the Contractors contract with the Authorized Recipient(s) and/or agreement with each authorized individual(s).

9.5 The Contractor shall submit payment to the FBI within thirty (30) calendar days from the bill date. Failure to pay may result in termination of the contract. Current FBI policy allows the Contractor one calendar year from the date the CJIS Division completed the fingerprint processing to request billing adjustments. If the Contractor is aware of a potential billing error before it receives the bill from the CJIS Division, e.g., the Contractor should contact the CJIS Division immediately at (304) 625-5590. Billing adjustments will be made on a limited and extenuating circumstance basis.

9.6 The Contractor who fails to submit payment as required above or is habitually late in paying the FBI shall be subject to immediate termination.

9.7 The Contractor shall develop instructions and information for dissemination to participating Authorized Recipients regarding the procedures to be followed to ensure the adequacy of the channeling system. This documentation should include the resolution of problems relating to, for example: (a) Incomplete or missing data on the applicant submissions, and/or illegible (i.e., unclassifiable) fingerprints; (b) Payment of fees, e.g., no payment, overpayment, underpayment, credit memorandums, etc.; (c) Reasonable inquiries by agencies and applicants regarding processing status of an applicant submission; and (d) Request for special or expedited processing based on extenuating circumstances. A copy of the instructions and information on the procedures to be followed by Authorized Recipients is to be enclosed in the proposal.

9.8 The Contractor shall provide all Authorized Recipients and/or authorized individuals with applicant fingerprint cards, if needed. The FBI no longer maintains a supply of applicant fingerprint cards for commercial dissemination.

9.9 The Contractor shall not submit a name check for an authorized individual(s) requesting a national noncriminal justice criminal history record check under the authority of the DO 556-73.

## 10. GOVERNMENT FURNISHED SERVICES

10.1 The FBI will authorize selected Contractors access to the FBI CJIS Division pursuant to Contract terms.

10.2 Should an existing Contractor (private or regulatory agency) elect to provide channeling services for other agencies/Authorized Recipients and/or authorized individuals outside its existing authority, it **MUST** respond to this RFP. Should an existing private or regulatory agency be selected by the FBI to serve as a Contractor under this initiative, then the agency shall provide and pay for all equipment (including maintenance) and telecommunication costs associated with the FBI CJIS Division connection in the same manner as other Contractors selected pursuant to this initiative.

10.3 The terms of this contract shall be in compliance with the Federal Acquisition Regulation.

#### 11.0 CONTRACTOR FURNISHED ITEMS

11.1 The Contractor shall provide and pay for all telecommunications equipment (including maintenance) and telecommunication costs associated with this contract.

11.2 The Contractor shall furnish all necessary labor, equipment, computers, scanners, printers, storage devices, supplies, consumable materials, and facilities necessary for the performance of the work of this contract.

#### 12.0 PLACE OF DELIVERY/PERFORMANCE

12.1 The Contractor shall maintain a facility of operations within any state, territory, or possession of the United States, the District of Columbia, or the Commonwealth of Puerto Rico. The Contractor will identify the facility as part of this RFP, and the location will not be changed during the contract except pursuant to a written agreement with the CJIS Division. All requests for a facility change shall be submitted to the COTR/TM in writing prior to occurrence. For further information regarding a change in location of the facility, contact the FBI COTR/TM.

#### 13.0 REQUIREMENTS FOR CONTRACTORS

13.1 The Contractor shall submit specific documentation to verify its ability to comply with the terms of this solicitation. Such information would include business location, ability to perform the technical services and security requirements, and examples of past performance services and the similarity of those services to the services required under this initiative. Additionally, the Contractor should describe whether it could perform administrative functions for other Authorized Recipients should the need arise.

13.2 The Contractor must describe the public liability and other forms of insurance it intends to carry for the duration of any resulting contract.

13.3 No person on the ground of disability, age, race, color, religion, sex, national origin, or sexual orientation, will be excluded from participation in, or be denied benefits of, or be otherwise subjected to discrimination in the performance of the contract.

#### 14.0 CONTRACT TERMINATION

14.1 If the Contractor fails to properly perform its obligations under the Contract or violates any terms of the Contract, the FBI will have the right to immediately terminate the Contract.

14.2 If the Contractor does not submit payments on the FBI account within the required thirty (30) days, the FBI will have the right to immediately terminate the Contract. Any diversion of such fees may be the subject of a criminal prosecution. All criminal history record check results in the possession of the terminated Contractor must be immediately returned to the CJIS Division.

14.3 If the Contractor fails to comply with any applicable federal law or regulation, the FBI will have the right to immediately terminate the Contract.

#### 15.0 FBI RESPONSIBILITIES

15.1 The FBI will return the results of each fingerprint-based national criminal history record check electronically to the Contractor. The charges that appear on the bill will reflect those transactions that are completed.

15.2 The FBI will bill the Contractor monthly for applicant fingerprint submissions processed during the preceding month.

15.3 The FBI will charge a fee for the processing of applicant fingerprint submissions. The FBI will not charge the Contractor an additional fee for the first resubmission and reprocessing of illegible (i.e., unclassifiable) submissions and those that cannot be processed due to missing information. A fee will be charged for subsequent resubmissions of an applicant's fingerprints.

To avoid incurring an additional charge when resubmitting fingerprints electronically, the Contractor must follow the procedures provided in the EBTS. This procedure stipulates the guidelines to resubmit electronic fingerprints that were previously rejected. The Contractor must place the Transaction Control Number (field number 1.09) from the electronic fingerprint response of the original rejected submission in the Transaction Control Reference (field number 1.10) of the new submission. Failure to provide this information with the resubmission will result in the FBI charging the Contractor another user fee.

15.4 The FBI conducts periodic reviews to determine whether the level and/or structure of the fees need to be adjusted. If a change in the fee levels or structure for applicant fingerprint submissions is required, the FBI will notify the Contractor of the change at least ninety (90) days prior to the effective date of the change.

#### SECTION D – PACKAGING AND MARKING – N/A

#### SECTION E – INSPECTION AND ACCEPTANCE

Inspection and Acceptance of the services called for hereunder shall be performed in accordance with the documents as specified in Section C, Section 2, Applicable Documents.

Inspection and acceptance of Contractor services in accordance with Federal Acquisition Regulation clause 52.246-1, and any other provision specified in this task order. The Government reserves the right to conduct any inspection and test it deems reasonably necessary to assure that the services and supplies provided conform in all respects to the specifications. Services and supplies, which upon inspection are found not to be in conformance with contractual specifications, shall be promptly rejected and notice of rejection, together with appropriate instructions, will be provided to the Contractor by the COTR.

FEDERAL ACQUISITION REGULATION TITLE

52.246-1 CONTRACTOR INSPECTION REQUIREMENTS (APR 1984)

The Contractor is responsible for performing or having performed all inspections and tests necessary to substantiate that the supplies or services furnished under this contract conform to contract requirements, including any applicable technical requirements for specified manufacturers' parts. This clause takes precedence over any Government inspection and testing required in the contract's specifications, except for specialized inspections or tests specified to be performed solely by the Government.

(End of clause)

SECTION F – DELIVERIES OR PERFORMANCE – See Section C

FEDERAL ACQUISITION REGULATION REFERENCE TITLE

(1) 52.242-15 STOP-WORK ORDER (AUG 1989)

SECTION G – CONTRACT ADMINISTRATION DATA

G.1 The Contractor shall comply with the terms and conditions of this contract.

G.2 CONTRACTING OFFICER'S TECHNICAL REPRESENTATIVE (COTR)/TASK MANAGER (TM):

[REDACTED]

Federal Bureau of Investigation  
Criminal Information and Transition Unit  
Module B-3  
1000 Custer Hollow Road  
Clarksburg, WV 26306  
Phone: [REDACTED]  
Fax: (304) 625-2539  
Email: [REDACTED]

b6  
b7c



G.3 CONTRACTING OFFICER (CO):

[REDACTED]

Federal Bureau of Investigation  
Information Technology Contracts Unit  
Module E-3  
1000 Custer Hollow Road  
Clarksburg, WV 26306  
Phone: [REDACTED]  
Fax: (304) 625-5391  
Email: [REDACTED]

G.4 FBI COMPACT OFFICER:



Federal Bureau of Investigation  
Criminal Information and Transition Unit  
Module D-3  
1000 Custer Hollow Road  
Clarksburg, WV 26306  
Phone   
Fax: (304) 625-2868  
Email: 

b6  
b7C

SECTION H – SPECIAL CONTRACT REQUIREMENTS

H.1 The Contractor shall comply with the terms and conditions of this contract. In addition, see Section C - Statement of Work.

H.2 All Contractor labor, equipment, computers, scanners, printers, storage devices, supplies, consumable materials, and facilities that contain FBI information or data, or that are generated by tasked efforts, shall be solely dedicated to FBI-tasks efforts, except as specifically approved by the FBICJIS COTR/TM or his/her designee in writing.

H.3 PERSONNEL

Requirements for personnel working on FBI tasks are described below.

H.3.1 General Personnel Requirements

Upon the award of the contract, appropriate Contractor individuals will be processed as directed by FBI policies and procedures. Section 5.12.1.1 of the FBI CJIS Security Policy provides that in order to verify identification, a state of residency and national fingerprint-based record checks shall be conducted within thirty (30) days of assignment for all personnel who have direct access to CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI. Such access will be coordinated through the FBI Compact Office, specifically the COTR/TM of this contract.

H.3.1.1 The following requirements shall be met by Contractor personnel working under this contract effort.

- All Contractor personnel shall be citizens of the United States.
- All Contractor personnel shall have, for three of the five years immediately prior to working on this effort:  
(1) resided in the United States; (2) worked for the United States overseas in a Federal or military capacity;  
or (3) be a dependent of a federal or military employee serving overseas.

H.3.2 Personnel Security and Access Requirements

H.3.2.1 If a felony conviction of any kind exists, the hiring authority in the Contractor's office shall deny systems access.

H.3.2.2 If a record of any other kind exists, systems access shall not be granted until the Security Programs Manager (SPM) or his/her official designee reviews the matter to determine if systems access is appropriate.

H.3.2.3 If the person appears to be a fugitive or appears to have an arrest history without conviction for a felony or serious misdemeanor, the SPM or his/her official designee shall review the matter to determine if systems access is appropriate.

H.3.2.4 If the person already has systems access from another law enforcement agency, e.g., shared dispatchers, the SPM or his/her designee may grant systems access prior to the confirmation of the new state of residency and national fingerprint-based record check.

H.3.2.6 Support personnel, contractors, and custodial workers who access computer terminal areas shall be subject to a state of residency and national fingerprint-based record check, unless these individuals are escorted by authorized personnel at all times.

For your information:

- ✓ "Authorized personnel" are those persons who have passed a state and national fingerprint-based record check and have been granted access.

### H.3.3 Security Incidents and Violations

H.3.3.1. Contractors shall identify a POC to manage security incidents and violations on their network accessing FBI CJIS data following award.

Because security incidents and violations can have many possible consequences that range from slight to catastrophic, priorities must be considered when evaluating and dealing with incidents. The following five priorities have been outlined:

- Priority 1 - Protect human life and people's safety.
- Priority 2 - Protect classified data.
- Priority 3 - Protect Sensitive But Unclassified data.
- Priority 4 - Prevent damage to systems (loss or alteration of system software and files, damage to disk drives, etc.).
- Priority 5 - Minimize disruption of computing resources.

### H.3.3.2 Incident Response Capability Structure

#### H.3.3.2.1 FBI CJIS Division Responsibilities

FBI CJIS Division responsibilities shall include:

- (a) Managing and maintaining the CJIS Division's Computer Security Incident Response Capability (CSIRC);
- (b) Serving as a central clearinghouse for all reported intrusion incidents, security alerts, bulletins, and other security-related material;
- (c) Ensuring additional resources for all incidents affecting FBI CJIS Division controlled systems as needed;
- (d) Disseminating prompt advisories of system threats and operating system vulnerabilities to the POC through an identified email account established for that purpose. These advisories include Product Security Bulletins, Virus Bulletins, and Security Clips;
- (e) Tracking all reported incidents and/or trends; and
- (f) Monitoring the resolution of all incidents.

### H.3.3.2.2 Contractor POC Responsibilities

Contractor POC responsibilities for security incidents shall include:

- (a) Assigning an individual to be the primary POC for interfacing with the FBI CJIS Division concerning incident handling and response;
- (b) Identifying individuals who are responsible for reporting incidents within their area of responsibility;
- (c) Collecting incident information from those individuals for coordination and sharing among other organizations that may or may not be affected by the incident;
- (d) Developing, implementing, and maintaining internal incident response procedures and coordinating those procedures with other organizations that may or may not be affected;
- (e) Collecting and disseminating all incident-related information received from the Department of Justice (DOJ), FBI CJIS Division, and other entities to the appropriate local law enforcement POCs within their area.
- (f) Acting as a single POC for their jurisdictional area for requesting incident response assistance.

## H.5 PUBLICATIONS

### Release of Information - Publications by Contractor Personnel

The FBI specifically requires that Contractors shall not divulge, publish, or disclose information or produce material acquired or derived from the performance of their duties.

For purposes of this Clause, "Information" shall include but not be limited to: in any media or all media including on the web or web sites; publications, studies, books, theses, photographs, films or public announcements, press releases describing any part of the subject matter of this contract or any phase of any program hereunder, except to the extent such is:

- (i) already known to the Contractor prior to the commencement of the contract
- (ii) required by law, regulation, subpoena or government or judicial order to be disclosed, including the Freedom of Information Act.

No release of information shall be made without the prior written consent of the Office of Public Affairs and the Contracting Officer. The contractor and author are warned that disclosure is not without potential consequences. The FBI will make every effort to review proposed publications in a timely manner to accommodate these and other publications.

Where appropriate, in accordance with established academic publishing practices, the FBI reserves the right to author/co-author any publication derived from this contract.

These obligations do not cease upon completion of the contract.

## H.6 CONTRACT TYPE

A Purchase Order will not be issued for the award of this contract. A SF-33 will be executed and valid for a one year base period with four exercisable one-year option periods.

## H.7 TRAVEL

All Contractor travel will be the responsibility of the Contractor. The FBI will not reimburse the Contractor for any travel associated with this contract.

## H.8 NEED-TO-KNOW

The primary security principle in safeguarding classified and sensitive information is to ensure it is accessible only by those persons with an appropriate clearance, access approval, clearly identified need-to-know, and an appropriate indoctrination. The holder of the information is expected to practice need-to-know discipline in disseminating or disclosing information about the program or project involved. Intrinsic to this discipline is acquiring or disseminating only that information essential to effectively carrying out the assignment. No person will be deemed to have a need-to-know solely by virtue of rank, title, or position.

## H.9 USE AND DISSEMINATION OF CHRI

### H.9.1 Terminology

CHRI is considered sensitive but unclassified information.

### H.9.2 Proper Access To, Use, and Dissemination of FBI CJIS System Information

#### H.9.2.1 Proper Access To and Use of CHRI

The CHRI may only be accessed for an authorized purpose. CHRI may only be used for an authorized purpose, consistent with the purpose for which the FBI CJIS system was accessed. Dissemination to another agency is authorized if (a) the other agency is an authorized recipient of such information and is being serviced by the accessing agency, or (b) is consistent with the "Related Agency Doctrine."

### H.9.3 Penalization

#### H.9.3.1 Improper Use of CHRI

CJIS systems data is sensitive information and security shall be afforded to prevent any unauthorized access, use, or dissemination of the information. Improper access, use and dissemination of CHRI is a serious offense and may result in the imposition of administrative sanctions including, but not limited to, termination of services and state and federal criminal penalties.

### H.9.4 Transfers of FBI CJIS CHRI via the Internet

The transfer of FBI CJIS CHRI by using the Internet and associated electronic media such as mail facilities, remote access file transfers, and any other file modifications shall be permitted provided all technical security requirements have been met. The Contractor will not knowingly support the use of the DO 556-73 process for licensing and employment matters.

### H.9.5 Facsimile Transmissions

CHRI may be transmitted via a facsimile device which is not connected to a CJIS system as long as both agencies involved in the transmission have an authorized ORI number. Prior to the transmission, the sending agency shall verify the receiving agency's authenticity.

### H.9.6 Dissemination Procedures

The Contractor shall develop instructions and information for dissemination to participating Authorized Recipients regarding the procedures to be followed to ensure the adequacy of the channeling system. This documentation should include the resolution of problems relating to, for example: (a) Incomplete or missing data on the applicant

submissions, and/or illegible (i.e., unclassifiable) fingerprints; (b) Payment of fees, e.g., no payment, overpayment, underpayment, credit memorandums, etc.; (c) Reasonable inquiries by agencies and applicants regarding processing status of an applicant submission; and (d) Request for special or expedited processing based on extenuating circumstances.

## SECTION I – CONTRACT CLAUSES

The DOJ does not permit the use of Non-U.S. Citizens in the performance of this contract. Furthermore, Contractor personnel must be a citizen of the United States and must have resided within the United States for three of the five years immediately prior to the issuance of this task order.

### FEDERAL ACQUISITION REGULATION REFERENCE TITLE

- |      |           |   |
|------|-----------|---|
| (1)  | 52.202-1  | DEFINITIONS (JUL 2004)  |
| (2)  | 52.204-3  | TAXPAYER IDENTIFICATION (OCT 1998)  |
| (3)  | 52.204-7  | CENTRAL CONTRACTOR REGISTRATION (APRIL 2008)  |
| (4)  | 52.204-8  | ANNUAL REPRESENTATIONS AND CERTIFICATIONS (JAN 2011)  |
| (5)  | 52.209-5  | CERTIFICATION REGARDING DEBARMENT, SUSPENSION, PROPOSED DEBARMENT,<br>AND OTHER RESPONSIBILITY MATTERS (APRIL 2010) |
| (6)  | 52.204-6  | DATA UNIVERSAL NUMBERING SYSTEM (DUNS) NUMBER (OCT 1993)  |
| (7)  | 52.215-1  | INSTRUCTIONS TO OFFERORS – COMPETITIVE ACQUISITION (JAN 2004)   |
| (8)  | 52.215-6  | PLACE OF PERFORMANCE (OCT 1997)   |
| (9)  | 52.217-8  | OPTION TO EXTEND SERVICES (NOV 1999)  |
| (10) | 52.222-21 | PROHIBITION OF SEGREGATED FACILITIES (FEB 1999)   |
| (11) | 52.222-26 | EQUAL OPPORTUNITY (MAR 2007)  |
| (12) | 52.224-1  | PRIVACY ACT NOTIFICATION (APR 1984)   |
| (13) | 52.224-2  | PRIVACY ACT (APR 1984)  |
| (14) | 52.233-1  | DISPUTES (JUL 2002)   |
| (15) | 52.233-2  | SERVICE OF PROTEST (SEPTEMBER 2006)   |
| (16) | 52.233-4  | APPLICABLE LAW FOR BREACH OF CONTRACT CLAIM (OCT 2004)  |
| (17) | 52.243-2  | CHANGES – COST-REIMBURSEMENT (AUG 1987)   |
| (18) | 52.243-2  | ALTERNATE I (APR 1984)  |
| (19) | 52.249-4  | TERMINATION FOR CONVENIENCE OF THE GOVERNMENT (SERVICES) (SHORT FORM)<br>(APR 1984)                                 |
| (20) | 52.249-6  | TERMINATION (COST-REIMBURSEMENT) (MAY 2004)   |
| (21) | 52.252-1  | SOLICITATION PROVISIONS INCORPORATED BY REFERENCE (FEB 1998)  |
| (22) | 52.252-2  | CLAUSES INCORPORATED BY REFERENCE (FEB 1998)  |
| (23) | 52.252-3  | ALTERATIONS IN SOLICITATION. (APR 1984)   |
| (24) | 52.253-1  | COMPUTER GENERATED FORMS (JAN 1991)   |

### 52.204-7 CENTRAL CONTRACTOR REGISTRATION (CCR) (APRIL 2008)

The DOJ requires that all Contractors shall be registered in the CCR database prior to award of contract or agreement.

(End of clause)

### 52.233-2 SERVICE OF PROTEST (SEPTEMBER 2006)

(a) Protests, as defined in section 33.101 of the Federal Acquisition Regulation, that are filed directly with an agency, and copies of any protests that are filed with the Government Accountability Office (GAO), shall be served

on the Contracting Officer (addressed as follows) by obtaining written and dated acknowledgment of receipt from ☐  
☐ [Contracting Officer designate the official or location where a protest may be served on the  
Contracting Officer.]

b6  
b7C

(b) The copy of any protest shall be received in the office designated above within one day of filing a protest with the GAO.

(End of provision)

#### 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es):

-----  
-----  
-----

[Insert one or more Internet addresses]

(End of clause)

#### 52.252-3 ALTERATIONS IN SOLICITATION. (APR 1984)

Portions of this solicitation are altered as follows:

-----  
-----  
-----

(End of provision)

#### SECTION J – LIST OF ATTACHMENTS (AND ENCLOSURES)

- Deliverables
- Appendix J of the FBI CJIS Security Policy
- 12/16/2004 Outsourcing of Noncriminal Justice Administrative Functions Interim Final Rule - Adopted as a Final Rule on 12/15/2005 and codified at 28 CFR § 906.
- November 3, 2010 version of the Security and Management Control Outsourcing Standard for Channelers
- February 9, 2011 version 5 of the FBI CJIS Security Policy

#### SECTION K – REPRESENTATIONS, CERTIFICATIONS, AND OTHER STATEMENTS OF CONTRACTORS OR RESPONDENTS

All representations, certifications, and other statements of this contract shall apply. Additionally, the following shall apply:

## FEDERAL ACQUISITION REGULATION REFERENCE TITLE

### (1) 52.215-6 PLACE OF PERFORMANCE (OCT 1997)

### 52.204-3 TAXPAYER IDENTIFICATION (OCT 1998)

#### (a) Definitions.

“Common parent,” as used in this provision, means that corporate entity that owns or controls an affiliated group of corporations that files its Federal income tax returns on a consolidated basis, and of which the contractor is a member.

“Taxpayer Identification Number (TIN),” as used in this provision, means the number required by the Internal Revenue Service (IRS) to be used by the offeror in reporting income tax and other returns. The TIN may be either a Social Security Number or an Employer Identification Number.

(b) All contractors must submit the information required in paragraphs (d) through (f) of this provision to comply with debt collection requirements of 31 U.S.C. 7701(c) and 3325(d), reporting requirements of 26 U.S.C. 6041, 6041A, and 6050M, and implementing regulations issued by the IRS. If the resulting contract is subject to the payment reporting requirements described in Federal Acquisition Regulation (FAR) 4.904, the failure or refusal by the contractor to furnish the information may result in a 31 percent reduction of payments otherwise due under the contract.

(c) The TIN may be used by the Government to collect and report on any delinquent amounts arising out of the contractor’s relationship with the Government (31 U.S.C. 7701(c)(3)). If the resulting contract is subject to the payment reporting requirements described in FAR 4.904, the TIN provided hereunder may be matched with IRS records to verify the accuracy of the contractor’s TIN.

#### (d) Taxpayer Identification Number (TIN).

- o TIN: \_\_\_\_\_.
- o TIN has been applied for.
- o TIN is not required because:
  - o Contractor is a nonresident alien, foreign corporation, or foreign partnership that does not have income effectively connected with the conduct of a trade or business in the United States and does not have an office or place of business or a fiscal paying agent in the United States;
  - o Contractor is an agency or instrumentality of a foreign government;
  - o Contractor is an agency or instrumentality of the Federal Government.

#### (e) Type of organization.

- o Sole proprietorship;
- o Partnership;
- o Corporate entity (not tax-exempt);
- o Corporate entity (tax-exempt);
- o Government entity (Federal, State, or local);
- o Foreign government;
- o International organization per 26 CFR 1.6049-4;
- o Other \_\_\_\_\_.

#### (f) Common parent.

- o Contractor is not owned or controlled by a common parent as defined in paragraph (a) of this provision.

o Name and TIN of common parent:

Name \_\_\_\_\_

TIN \_\_\_\_\_

(End of provision)

52.204-8 ANNUAL REPRESENTATIONS AND CERTIFICATIONS (JAN 2011)

(a)(1) The North American Industry Classification System (NAICS) code for this acquisition is \_\_\_\_\_ [insert NAICS code].

(2) The small business size standard is \_\_\_\_\_ [insert size standard].

(3) The small business size standard for a concern which submits an offer in its own name, other than on a construction or service contract, but which proposes to furnish a product which it did not itself manufacture, is 500 employees.

(b)(1) If the clause at 52.204-7, Central Contractor Registration, is included in this solicitation, paragraph (c) of this provision applies.

(2) If the clause at 52.204-7 is not included in this solicitation, and the contractor is currently registered in CCR, and has completed the ORCA electronically, the contractor may choose to use paragraph (c) of this provision instead of completing the corresponding individual representations and certifications in the solicitation. The contractor shall indicate which option applies by checking one of the following boxes:

☐ (i) Paragraph (c) applies.

☐ (ii) Paragraph (c) does not apply and the contractor has completed the individual representations and certifications in the solicitation.

(c) The contractor has completed the annual representations and certifications electronically via the Online Representations and Certifications Application (ORCA) website at <http://orca.bpn.gov>. After reviewing the ORCA database information, the contractor verifies by submission of the offer that the representations and certifications currently posted electronically have been entered or updated within the last 12 months, are current, accurate, complete, and applicable to this solicitation (including the business size standard applicable to the NAICS code referenced for this solicitation), as of the date of this offer and are incorporated in this offer by reference (see FAR 4.1201); except for the changes identified below [contractor to insert changes, identifying change by clause number, title, date]. These amended representation(s) and/or certification(s) are also incorporated in this offer and are current, accurate, and complete as of the date of this offer.

FAR CLAUSE #	TITLE	DATE	CHANGE
--------------	-------	------	--------

_____	_____	_____	_____
-------	-------	-------	-------

Any changes provided by the contractor are applicable to this solicitation only, and do not result in an update to the representations and certifications posted on ORCA.

(End of provision)

52.209-5 CERTIFICATION REGARDING DEBARMENT, SUSPENSION, PROPOSED DEBARMENT, AND OTHER RESPONSIBILITY MATTERS (APRIL 2010)

(a)(1) The Offeror certifies, to the best of its knowledge and belief, that—

(i) The Offeror and/or any of its Principals—

(A) Are ☐ are not ☐ presently debarred, suspended, proposed for debarment, or declared ineligible for the award of contracts by any Federal agency;

(B) Have ☐ have not ☐, within a three-year period preceding this offer, been convicted of or had a civil judgment rendered against them for: commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (Federal, state, or local) contract or subcontract; violation of Federal or state antitrust statutes relating to the submission of offers; or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, tax evasion, or receiving stolen property; and

(C) Are ☐ are not ☐ presently indicted for, or otherwise criminally or civilly charged by a governmental entity with, commission of any of the offenses enumerated in paragraph (a)(1)(i)(B) of this provision.

(D) Have ☐ have not ☐, within a three-year period preceding this offer, been notified of any delinquent Federal taxes in an amount that exceeds \$3,000 for which the liability remains unsatisfied.

(ii) The Offeror has ☐ has not ☐, within a three-year period preceding this offer, had one or more contracts terminated for default by any Federal agency.

(2) "Principals," for the purposes of this certification, means officers; directors; owners; partners; and, persons having primary management or supervisory responsibilities within a business entity (e.g., general manager; plant manager; head of a subsidiary, division, or business segment, and similar positions).

This Certification Concerns a Matter Within the Jurisdiction of an Agency of the United States and the Making of a False, Fictitious, or Fraudulent Certification May Render the Maker Subject to Prosecution Under Section 1001, Title 18, United States Code.

(b) The Offeror shall provide immediate written notice to the Contracting Officer if, at any time prior to contract award, the Offeror learns that its certification was erroneous when submitted or has become erroneous by reason of changed circumstances.

(c) A certification that any of the items in paragraph (a) of this provision exists will not necessarily result in withholding of an award under this solicitation. However, the certification will be considered in connection with a determination of the Offeror's responsibility. Failure of the Offeror to furnish a certification or provide such additional information as requested by the Contracting Officer may render the Contractor nonresponsible.

(d) Nothing contained in the foregoing shall be construed to require establishment of a system of records in order to render, in good faith, the certification required by paragraph (a) of this provision. The knowledge and information of an Offeror is not required to exceed that which is normally possessed by a prudent person in the ordinary course of business dealings.

(e) The certification in paragraph (a) of this provision is a material representation of fact upon which reliance was placed when making award. If it is later determined that the Offeror knowingly rendered an erroneous certification, in addition to other remedies available to the Government, the Contracting Officer may terminate the contract resulting from this solicitation for default.

(End of provision)

## SECTION L – INSTRUCTIONS, CONDITIONS, AND NOTICES TO CONTRACTOR

### L.1 FORMAT AND INSTRUCTIONS FOR PROPOSALS

The proposal submitted in response to this RFP shall be formatted as follows. A cover letter may accompany the proposal to set forth any information that the Contractor wishes to bring to the attention of the Government.

The Contractors shall provide one (1) CD and four (4) hard copies of the proposal, which shall be submitted no later than 2:00 p.m. Eastern Standard Time on September 3, 2011. Proposals are to be no longer than 25 pages in length and must be single sided. No e-mail proposals will be accepted.

In order to have an acceptable proposal, the Contractor must meet all of the requirements as set forth in Section C – Statement of Work. Each Contractor is encouraged to provide only information relevant to the RFP. Elaborate brochures or documentation, binding, detailed artwork, or other embellishments are unnecessary and are not desired.

In order to ensure complete evaluation of each Contractor's technical merit, proposals must specify the technical approach proposed to satisfy the requirements and not merely paraphrase the specifications contained in the RFP. It is essential that Contractors clearly demonstrate in their technical proposal that they have the capability, experience, and necessary personnel required to furnish the services stipulated herein.

No vendor library will be established. All applicable documents are provided on the internet or as an attachment, except for the documents as specified in Section C, 4.1.3.

Any questions will be addressed at the discretion of the CO. Electronic submission of questions is the only acceptable method of submission. The Government will not provide any answers to questions by telephone or fax. Submit electronically any questions via e-mail to [REDACTED] at [REDACTED]. All questions must be received by August 17, 2011, to ensure answers.

b6  
b7C

### FEDERAL ACQUISITION REGULATION REFERENCE TITLE

52.246-2 52.204-6 DATA UNIVERSAL NUMBERING SYSTEM (DUNS) NUMBER (OCT 1993)

52.246-3 52.215-1 INSTRUCTIONS TO OFFERORS – COMPETITIVE ACQUISITION (JAN 2004)

52.246-4 52.252-1 SOLICITATION PROVISIONS INCORPORATED BY REFERENCE (FEB 1998)

## SECTION M - EVALUATION FACTORS FOR AWARD

### M.1 EVALUATION

M.1.1. The Government will authorize FBI CJIS Division connections resulting from this solicitation to one or multiple Contractors whose offers, conforming to the solicitation, best satisfy the Government's requirements. The selection of Contractors shall be in accordance with Paragraph M.3 below.

M.1.2. A written notice of award or acceptance of an offer, mailed or otherwise furnished to the successful Contractor(s) within the time for acceptance specified in the offer, shall result in a binding contract. Before the Contractor's specified expiration time of 30 days, the Government may accept an offer (or part of an offer) without discussions unless a written notice of withdrawal is received before award. The Government specifically reserves the right to remove from award consideration any proposal that does not conform to all requirements in the solicitation.

## M.2 PRE-AWARD SURVEY

The Government may conduct a complete or partial pre-award survey of prospective Contractors. The following factors may be investigated during the survey and any findings will be considered in the evaluation process:

- (a) Technical Capability
- (b) Financial Capability
- (c) Accounting System
- (d) Quality Assurance Capability
- (e) Labor Resource
- (f) Performance Record
- (g) Ability to meet required schedule
- (h) Ability to provide the required services
- (i) Security Clearance

## M.3 BASIS OF AWARD

M.3.1. The following conditions must be met in order to be eligible for award:

M.3.1.1. The proposal must comply in all material respects with the requirements of law, regulation, and conditions set forth in the solicitation. Additionally, Contractors are encouraged to comment upon their abilities to perform channeling duties, the amount of work they are competent to perform, expected sources of work, and whether they are available to accept fingerprint submissions from additional Authorized Recipients.

M.3.1.2. The Contractor must be determined to be responsible according to the standards in Federal Acquisition Regulation Subpart 9.1.

M.3.1.3. Upon satisfying the above conditions, the Source Selection Authority will determine the proposals that satisfy the Government's requirements. The selections will be based on how well each proposal satisfies the evaluation criteria as described in Paragraph M.4. For evaluation purposes, the area of Technical Services will be significantly more important than Past Performance.

### M.3.2 Other Evaluation Information

M.3.2.1 In conducting evaluations of proposals, the Government reserves the right to utilize all information available at the time of evaluations. The Government may rely on information contained in its own records (such as Government audit agencies), commercial sources (such as Dunn and Bradstreet Reports), and information publicly available (such as information available on the Internet). If information obtained through outside sources substantially disagrees with the Contractor's proposal, the Contractor will be given an opportunity to address the inconsistencies.

M.3.2.2 The Government reserves the right to award one or multiple contracts that will strive to strike a balance between the number of Contractors it has the capability to administer and the number needed to effectively and efficiently serve the needs of Authorized Recipients.

## M.4 EVALUATION CRITERIA

### M.4.1 General

The evaluation will be based on an integrated assessment of the information submitted in the Contractor's proposal and other evaluation information available to the Government. The integrated assessment will evaluate past

performance, mandatory requirements, terms and conditions, and technical factors. This assessment will specifically evaluate two areas: Technical Services and Past Performance.

#### M.4.2 Risk Assessment

The integrated assessment of proposals will include a risk assessment for the overall Technical Services and Past Performance areas. The Government will assess the risk associated with the Contractor's proposal for performance.

#### M.4.3 Relative Order of Importance of Evaluation Areas

For evaluation purposes, the area of Technical Services will be significantly more important than Past Performance. Within the Technical Services and Past Performance areas, factors have equal importance.

#### M.4.4 Specific Criteria for Evaluation

The following paragraphs address the specific evaluation criteria for the Technical Services and Past Performance areas.

**M.4.4.1 AREA: Technical Services.** The Technical Services Area assesses the Contractor's ability to provide effective technical services with respect to the following factors: Sustained Customer Base, Infrastructure, Financial – Billing, and Transaction Processing.

**M.4.4.1.1 FACTOR: Sustained Customer Base.** Assesses the Contractor's ability to service multiple contracts and industries in multiple states. Also assesses the ability to respond quickly to new Federal and state legislation requiring fingerprint-based national criminal history record checks, DO 556-73 requests, and PROTECT Act submissions. The Contractor shall submit the following:

- (a) years and breadth of experience as a Contractor, including store and forward capability;
- (b) the number of fingerprints the entity/agency is capable of submitting, to the FBI annually;
- (c) the number of fingerprint submissions the Contractor expects to submit to the FBI annually and the basis for the estimate;
- (d) whether the Contractor plans to service the channeling needs of a specific industry to which the Contractor is affiliated or plans to pursue expanding its service to other industries that submit fingerprints to the FBI;
- (e) a list of potential customers that are Authorized Recipients of FBI-maintained CHRI.

**M.4.4.1.2 FACTOR: Infrastructure.** Assesses the Contractor's ability to support an adequate infrastructure to service multiple contracts and industries in multiple states. Also assesses the ability to respond quickly to new Federal and state legislation requiring fingerprint-based national criminal history record checks, DO 556-73 requests, and PROTECT Act submissions. The Contractor shall address its ability to satisfy Sections 4, 8.1, 8.2, 8.3, 8.6, 11.1, and H of the SOW with respect to the following:

- (a) obtaining, identifying, and maintaining secure facilities;
- (b) obtaining and maintaining telecommunication and network equipment and resources;
- (c) obtaining and maintaining IT equipment and resources (i.e., hardware, software, maintenance agreements);
- (d) hiring and retaining qualified personnel;
- (e) detailed description of plans, procedures, and resources to support continuity of operations;
- (f) detailed description of plans, procedures, and resources to maintain appropriate transaction history and audit files.

M.4.4.1.3 FACTOR: Financial – Billing. Assesses the Contractor's ability to meet requirements as specified in Sections 8.4, 8.5, and 8.6 of the SOW.

M.4.4.1.4 FACTOR: Transaction Processing. Assesses the Contractor's ability to provide fingerprint processing services for multiple contracts and industries in multiple states. Also assesses the ability to respond quickly to new Federal and state legislation requiring fingerprint-based national criminal history record checks, DO 556-73 requests, and PROTECT Act submissions. The Contractor shall address its ability to satisfy Sections 4, 8, 11.1, and H of the SOW with respect to the following:

- (a) receiving, logging, and processing fingerprint requests (transactions) from Authorized Recipients;
- (b) submitting and logging compliant fingerprint transactions to CJIS Division;
- (c) receiving, logging, and processing transaction responses from CJIS Division;
- (d) disseminating and logging fingerprint responses to Authorized Recipients;
- (e) establishing and maintaining data to support transaction tracking and reporting transaction statistics to facilitate CJIS Audits;
- (f) establishing and maintaining a quality assurance program.

M.4.4.2 AREA: Past Performance. The Past Performance area assesses the performance record of the Contractor with respect to Experience and Customer Satisfaction.

M.4.4.2.1 FACTOR: Experience. Assesses the Contractor's experience in the fingerprint processing field. The Contractor shall submit a detailed narrative specifying how its experience will be used to facilitate the receipt, handling, and prompt electronic submission of applicant fingerprint submissions to the FBI, the receipt of fingerprint search results, and the dissemination of the results to the Authorized Recipient. Also, the Contractor shall provide three examples of its experience within the past three (3) years with the following:

- (a) fingerprint capture (hard copy or electronic);
- (b) fingerprint transmittal of hard copy or electronic fingerprints (currently serves as Contractor or provides store and forward capability);
- (c) electronic conversion of hard copy fingerprints to digitized images meeting FBI's image quality specifications.

The Contractor shall provide the name and phone numbers of individuals to verify each example provided.

The Contractor shall also describe its current (or recent) contract activities that involve:

- (a) commercial background check services, including, criminal history background checks, and the dissemination of the results of such checks to multiple clients;
- (b) describe the company's products that are (or have been) certified for compliance with the FBI's IAFIS Image Quality Specifications.

In evaluating this Factor, the Government may assess Contractor supplied information, current government information and experience related to the Contractor, and information developed as a result of direct contact with current and previous users of the Contractor's services.

M.4.4.2.2 FACTOR: Customer Satisfaction. The Customer Satisfaction Factor will assess, from a customer's perspective, the Contractor's record of satisfying customer needs, to include the Contractor's record of professionalism in dealing with customers. The factor will address services performance and management and support personnel performance.

In evaluating this factor, the Government may assess Contractor supplied information, current government information and experience related to the Contractor, and information developed as a result of direct contact with current and previous users of the Contractor's services.

M4.4.2.2.1 Services Performance. This factor will assess, from a customer's perspective, the Contractor's experience providing timely, effective, responsive, and quality services.

M4.4.2.2.2 Management and Support Personnel Performance. This factor will assess, from a customer's perspective, the Contractor's experience providing management and support personnel who are qualified and innovative.

## DELIVERABLES

The Contractor shall provide the following deliverables to the COTR/TM or his/her designee as directed by the requirements in this RFP or as requested by the COTR/TM. If the COTR/TM or his/her designee does not reply within 30 working days of receipt, the deliverables are to be considered to be acceptable.

- 1) Security Program - Section 4.2
- 2) Security Training Policy - Section 4.2.1.1
- 3) Biennial Training Notification - Sections 4.2.1.1 and 5.2.1.1
- 4) Contingency Plan (system security) - Section 4.2.5.4
- 5) Written Security Violation Policy – Section 4.2.6.1
- 6) Log Maintenance – Section 4.3.4
- 7) Request and Prior Approval for Subcontractor(s) – Section 7.5
- 8) Dissemination Procedures – Section 8.6
- 9) Security Incident Point-of-Contact – Section H.3.3.1

## Appendix J of the FBI CJIS Security Policy

This supplemental guidance for noncriminal justice agencies (NCJA) is provided specifically for those whose only access to FBI CJIS data is authorized by legislative enactment or federal executive order to request civil fingerprint-based background checks for licensing, employment, or other noncriminal justice purposes, via their State Identification Bureau and/or Channeling agency. This guidance does not apply to criminal justice agencies covered under an active user agreement with the FBI CJIS Division for direct connectivity to the FBI CJIS Division via the FBI CJIS Wide Area Network. Examples of the target audience for this supplemental guidance include school boards, banks, medical boards, gaming commissions, alcohol and tobacco control boards, social services agencies, pharmacy boards, etc. The information below identifies the sections of the FBI CJIS Security Policy most closely related to the NCJA's limited scope of interaction with criminal justice information (CJI).

The following FBI CJIS Security Policy sections comprise the minimum standard requirements in all situations:

- a. 3.2.9 – Local Agency Security Officer (LASO)
- b. 5.1.1.6 – Agency User Agreements
- c. 5.1.1.7 – Security and Management Control Outsourcing Standard\*
- d. 5.1.3 – Secondary Dissemination
- e. 5.2.1.1 – Security Awareness Training
- f. 5.3 – Incident Response
- g. 5.4.6 – Audit Record Retention
- h. 5.8 – Media Protection
- i. 5.9.2 – Controlled Area
- j. 5.11 – Formal Audits \*\*
- k. 5.12 – Personnel Security\*\*\*

\*Note: Outsourcing Standard applies when contracting with channeling or outsourcing agency.

\*\*Note: States shall periodically conduct audits of NCJAs. The FBI CJIS Division shall triennially conduct audits of a sampling of NCJAs.

\*\*\*Note: See the National Crime Prevention and Privacy Council's Outsourcing Standard for Contractor background check requirements.

2. Agencies located within states having passed legislation authorizing or requiring civil fingerprint-based background checks for personnel with access to criminal history record information for the purposes of licensing or employment shall follow the guidance in section 5.12. Agencies located within states without this authorization or requirement are exempted from the fingerprint-based background check requirement until such time as appropriate legislation has been written into law.

3. When receiving CJI via encrypted e-mail or downloading from a web-site and subsequently storing the information as an encrypted electronic image Authorized Recipients should, in addition to all of the aforementioned sections, focus on compliance with policy sections:

- a. 5.5.2.4 – Access Control – Encryption
- b. 5.6 – Identification and Authentication (web-site access)
- c. 5.10.1.2 – System and Communications Protection – Encryption

4. When receiving CJI via e-mail or retrieving CJI from a website and subsequently storing the CJI electronically, Authorized Recipients should, in addition to 1.a–1.k above, focus on compliance with policy sections:

- a. 5.5.2.4 – Access Control – Encryption
- b. 5.6 – Identification and Authentication

c. 5.7 – Configuration Management

d. 5.10 – System and Communications Protection and **Information Integrity**

5. If an NCJA further disseminates CJI via encrypted e-mail to Authorized Recipients, located outside the NCJA's designated controlled area, the NCJA should, in addition to 1.a–3.c above, focus on compliance with policy sections:

a. 5.7 – Configuration Management

b. 5.10 – System and Communications Protection and **Information Integrity**

6. If an NCJA further disseminates CJI via secure website posting to Authorized Recipients, located outside the NCJA's designated controlled area, the NCJA should focus on all sections outlined in 1.a-4.d above.